EXHIBIT AP

[PUBLIC VERSION]

FEDERAL RESERVE BANK of KANSAS CITY

October 21, 2022

Board of Directors
c/o Caitlin Long, CEO
Custodia Bank, Inc.
2120 Carey Avenue, Suite 300
Cheyenne, Wyoming 82001

EXHIBIT 109
WIT: Gingerton
DATE: 10-24-23
Peggy Corbett RDR, CSR, CRR, CCR

Via Electronic Mail: caitlin@custodiabank.com

Members of the Board:

As part of the ongoing efforts by the Federal Reserve Bank of Kansas City (Reserve Bank) to evaluate the application materials submitted by Custodia Bank, Inc., Cheyenne, Wyoming (Custodia), to become a member of the Federal Reserve System, an initial, pre-membership examination of Custodia commenced on September 6, 2022, and concluded on September 23, 2022. This letter is intended to memorialize our recent meetings and provide feedback on the issues identified through the course of our initial examination. As previously communicated, the information obtained during the examination and the Reserve Bank's assessment of Custodia's operations, activities, and risk profile are also informing the ongoing master account request evaluation process.

The scope of the review focused on imminent products and services to be offered by Custodia, including deposit taking, online banking services, Fedwire services, Automated Clearing House (ACH) services[1], and internal transfer activity, which Custodia defines in its business plan as its "core banking services." The examination included integrated reviews of various elements associated with the implementation of these core banking services, such as information technology and cybersecurity considerations, compliance with Bank Secrecy Act (BSA), Anti-Money Laundering (AML), and Office of Foreign Assets Control (OFAC)-imposed sanctions and regulatory requirements, audit procedures and internal controls, projected financial performance, and overall governance and risk management. The examination did not include a comprehensive assessment of any of Custodia's planned digital asset activities, as the technology and risk management infrastructures to support, facilitate, and execute these activities remain in the early stages of development.

Pre-membership Examination Results

Custodia has not yet begun operations and is actively developing policies and procedures in many areas. However, in accordance with Regulation H, Membership of State Banking Institutions in the Federal Reserve System, Appendix D-1, Interagency Guidelines Establishing Standards for Safety and Soundness, the pre-membership examination identified numerous exceptions to, or departures from, safe and sound banking practices in Custodia's prospective risk management program compared to the risk management practices that would typically be expected

[1] In initial operations, Fedwire and ACH services are planned to be provided through a relationship with a partner bank.

or required of an operating state member bank under Reserve Bank supervision. These exceptions from standards, requirements, or best practices are referred to as "risk management gaps" for purposes of this letter. Significant risk management gaps were identified specific to overall risk management, the BSA/AML and OFAC compliance program, the information technology program, the internal audit program, and various financial areas. Certain gaps are outlined below, and more detailed gaps and feedback items were verbally communicated during meetings with Custodia held on October 12, 2022, and October 13, 2022.

Risk Management

The assessment of Custodia's risk management practices included a review of board of directors and senior management oversight; policies, procedures, and risk limits; risk monitoring and management information systems; and audit and internal controls. Examiners identified significant risk management gaps, which may, at least partially, be attributed to a lack of depth and breadth of expertise in risk, banking regulation, and compliance at the board of directors and management levels. In general, overall policies and procedures are limited in detail and are not sufficiently tailored to Custodia's unique business model and planned activities. Detailed processes are not formalized and are insufficiently developed in many areas. As of the examination, risk assessment processes were not yet well developed or supported, most notably for the areas of BSA/AML and OFAC compliance, internal audit, and information technology. Well-developed risk assessments are an essential component for identifying the need for, and evaluating the effectiveness of, risk-mitigating controls, as well as for guiding independent review activities. More detail on specific risk management gaps is outlined below. *Subsequent to the examination, Custodia hired a Senior Vice President of enterprise risk management; the Reserve Bank has not yet had an opportunity to evaluate the effectiveness of this individual in enhancing risk management practices.*

BSA/AML and OFAC Compliance

Examiners reviewed the BSA/AML and OFAC compliance program relative to core banking products and services that are planned to commence in the short term, such as deposit services and traditional payment services. The effectiveness of the BSA/AML and OFAC compliance program related to planned digital asset-related activities could not yet be assessed. Transaction testing could not be conducted as Custodia has not yet begun operations. Despite limitations in the scope of areas that could be reviewed during the examination, significant gaps were identified, indicating that management has not yet established a reasonably designed BSA/AML and OFAC compliance program.

Regulation H (12 CFR § 208.63) and 31 CFR § 1020.210 require banks to establish and maintain procedures reasonably designed to assure and monitor compliance with the BSA. Gaps were identified in the BSA/AML and OFAC compliance program related to the need for development and implementation of a comprehensive BSA/AML and OFAC compliance risk assessment; largely undocumented and/or insufficiently developed procedures and processes in many areas; a lack of oversight and implementation of key information technology systems and processes; and limitations in training. *Subsequent to the examination, management completed an*

updated BSA/AML and OFAC risk assessment. The sufficiency of the updated risk assessment and related support for its conclusions have not yet been evaluated by the Reserve Bank, and the assessment's effectiveness in guiding the development of a satisfactory BSA compliance program and control structure has not yet been validated.

Regulation H (12 CFR § 208.62) and 31 CFR § 1020.320 require the timely filing of Suspicious Activity Reports when a bank detects a known or suspected violation of Federal law, or a suspicious transaction related to money laundering or a violation of the BSA. While Custodia is not yet operating, gaps were identified in policies, procedures, and processes relative to the timely identification and reporting of suspicious activity. Transaction monitoring processes, as communicated to examiners, are not risk-based and do not align with Custodia's planned operations and the higher risks posed by the planned digital asset activities.

In addition to addressing and remediating the gaps related to the BSA/AML and OFAC compliance program outlined in this letter and verbally communicated to management, Custodia should establish a broader plan for ensuring adequate resources are allocated to the development, implementation, and oversight of a BSA/AML and OFAC compliance program that satisfactorily addresses immediate risks posed by its core banking services and future risks posed by planned products and services, including, but limited to, those related to crypto-assets.

While more detailed gaps were communicated at the conclusion of the examination, additional information related to the significant gaps identified in the BSA/AML and OFAC compliance program is as follows:

- A comprehensive BSA/AML and OFAC compliance risk assessment (including the identification and evaluation of internal controls for purposes of developing an appropriately risk-based BSA/AML and OFAC compliance program) had not yet been developed at the time of the examination. Prior documented risk assessment methodologies or frameworks did not appropriately address the varying degrees of risk associated with its products, services, customers, and geographic locations, nor contain sufficient detail to guide the development of an adequate BSA/AML and OFAC risk assessment and control structure. Improper identification and assessment of risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA/AML compliance program.
- Procedures and processes are largely undocumented or have not been sufficiently developed, and do not allow for program continuity in the event of changing operations, management, employee composition, or structure.
- Oversight of key information technology systems and processes (including implementation of available functionality and management's understanding of the functionality) to support BSA/AML and OFAC compliance is not evident.
- Training for all personnel, and most critically for BSA personnel, is not tailored to Custodia's risk profile and does not include sufficient material related to money laundering and terrorist financing risks specific to planned products, services, customers, and geographies.

- In the current state, customer due diligence policies, procedures, and processes do not allow Custodia to form an adequate understanding of the customer relationship for the purpose of developing a risk profile. As the related processes were described to examiners, insufficient information would be obtained for higher-risk customer types and due diligence information would not be sufficiently incorporated into the customer risk profile on an initial or ongoing basis.
- Processes and transaction monitoring systems for ongoing monitoring of higher risk customers appear insufficient to allow for the timely identification and reporting of suspicious transactions.

<u>Information Technology</u>

The examination of information technology (IT) included a review of IT audit, IT management, development and acquisition, and support and delivery. Significant gaps were identified relative to the development and formalization of comprehensive IT-related policies, procedures, and standards; the overall IT risk management framework; vendor management; and business continuity planning. *Subsequent to the examination, management submitted updated business continuity planning documents and a cybersecurity risk assessment. The sufficiency of the new documentation and related support has not yet been assessed by the Reserve Bank.*

While more detailed gaps were communicated to management at the conclusion of the examination, additional information related to the significant gaps identified related to IT is as follows:

- The Information Security and Technology Policy and the Vendor Management Policy include outdated or incorrect information. Related procedures and standards are not yet developed or documented in most areas.
- The IT risk management framework, including the regular completion of the various risk assessments, is not well defined. The IT risk assessment methodology does not ensure timely, well-supported risk assessments that reflect current business plans. Formalized risk assessments for products under development are not yet regularly updated to ensure risks are identified and that appropriate controls are considered and documented in advance of new products and services being initiated. As of the examination, formal risk assessments had not yet been conducted for most areas, including the overall IT environment, cybersecurity, and disaster recovery. Additionally, completed risk assessments for planned products and services are outdated and contain only limited support.
- Despite executed contracts, vendor risk assessments and due diligence have not yet been documented for most vendors. Furthermore, processes have not yet been developed relative to the regular review and reporting of vendor management information to the board of directors.
- As of the examination, business continuity planning was not risk-based and a business impact analysis had not been conducted.

Internal Audit

Examiners reviewed audit policy guidance, audit risk assessments and the audit universe, and preliminary audit and internal audit plans. Internal audits have not yet been conducted. However, significant gaps were identified within the internal audit program related to the designation of a competent and independent audit manager to oversee the outsourced internal audit program, as well as the separation of accounting firms conducting the outsourced internal and external audits, indicating a lack of independence. While these gaps may potentially be mitigated in the short term when the volume of projected activity remains low, plans should be developed to directly address these gaps as new products and services are introduced and the organization's risk profile and complexity evolve. Additional gaps were identified relative to the completeness of audit policy guidance and the audit risk assessment methodology.

While more detailed gaps were communicated at the conclusion of the examination, additional information related to the gaps identified within the internal audit program is as follows:

- Custodia has not designated a competent and independent audit manager to oversee the outsourced internal audit program. Oversight of Custodia's wholly outsourced internal audit program has been assigned to the chief compliance officer (CCO). The CCO has direct oversight of, and therefore lacks independence relative to, the BSA/AML and OFAC compliance program. Additionally, the CCO may not have the expertise to oversee the audit activities of other areas of review, such as IT.
- Custodia has engaged the same firm, albeit through different audit teams and statements of work, to conduct outsourced internal audits and the external audit of the financial statements, indicating an apparent lack of independence related to the outsourced audit firm.
- The audit policy does not address how Custodia will provide oversight of the outsourced internal audit service provider(s), ensure conformance with Institute of Internal Auditors (IIA) Standards, describe the risk assessment methodology employed, or define internal audit's reporting standards and expectations.
- The risk assessment methodology and processes used to determine the audit scope and audit review frequencies do not adequately define risk scoring and the rationale for risk ratings.
- Processes and activities that would be subject to continuous monitoring or auditing have not been identified in areas where continuous monitoring or auditing would be warranted, given the speed and finality of transactions Custodia intends to perform on behalf of its customers.

Financial Factors

Examiners identified gaps related to the various financial areas reviewed during the examination. While more detailed feedback was communicated to management at the conclusion of the examination, additional information related to liquidity risk management and projected earnings performance is as follows:

- Custodia has not yet developed liquidity policies or procedures, including, but not limited to, a contingency funding plan, liquidity risk management metrics, or comprehensive liquidity policy guidance.

- Financial projections show rapid and significant scaling to profitability but are highly dependent on widespread customer adoption of products and services, as well as acceptance of the proposed fee structure. While rapid revenue growth is projected, operating expenses are projected to remain relatively stable. Key assumptions driving projected fee income and related growth, combined with stable operating expenses, are not sufficiently supported. Absent rapid projected net income growth, additional capital raises may be necessary in future periods to meet minimum capital level commitments made to the Wyoming Division of Banking. Well supported financial projections would aid in supporting the planned viability of Custodia.

Conclusion

These matters, focused on core banking services to be offered in the near term, represent gaps that we would expect an applicant to address prior to becoming a state member bank, as they could result in heightened risks or deterioration in financial condition if not corrected. Moreover, Custodia's business strategy includes plans to offer crypto-asset-related products and services, including custody activities, issuance of a proprietary digital payment instrument recorded on a public blockchain (Avit), and "Prime Services[2]." During the review, examiners confirmed the technology and risk management infrastructures to support, facilitate, and execute these activities remain in the early stages of development. Consequently, there was insufficient information available at the time of the examination to fully evaluate the adequacy of Custodia's risk management systems and controls in enabling it to engage in the proposed activities in a safe and sound manner, or comprehensively assess the overall administration of these activities relative to the statutory factors the Federal Reserve is required to consider under Section 208.3 of Regulation H.

As Custodia continues efforts to address the matters referenced above and makes progress in developing the technology and risk management programs that will be used to execute its planned digital asset products/services and overall business plan in a safe and sound manner, the Reserve Bank, in coordination with staff of the Board of Governors of the Federal Reserve System, will continue to evaluate the application for membership. Once all the gaps identified at the examination have been addressed in totality, Custodia may provide a comprehensive written response to the Reserve Bank describing all corrective actions taken or planned, including any supporting documentation. These remediation efforts will subsequently be assessed by Reserve Bank staff at a future date, which may include onsite reviews/examinations and/or additional requests for information deemed necessary to evaluate the organization's application relative to the requirements within Regulation H. In the interim, the Reserve Bank will continue to engage in periodic discussions with Custodia's senior management regarding the status of its operations and other matters pertinent to the membership application. The information gained through these ongoing exchanges, coupled with Custodia's progress in addressing the gaps referenced above and further maturing its operations and risk management framework, will also inform the Reserve Bank's continuing analysis of Custodia's request for a master account, which remains under consideration at this time.

[2] At this time, planned "Prime Services" include the facilitation of customer digital asset purchase and sale activities (as agent), facilitation of lending customers' digital assets (as directed trustee), and foreign exchange services.

Any questions related to Custodia's request for membership in the Federal Reserve System may be directed to Vice President Judith Hazen at (816) 881-2789, Applications Senior Examiner Ben McGhee at (816) 881-2803, or me at (816) 881-2073.

Sincerely,

Jeff Imgarten

Jeff Imgarten
Assistant Vice President

cc: Board of Governors of the Federal Reserve System
Wyoming Division of Banking